FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Are you on the bus? Detecting relative position of devices versus mobile hotspots

Leonid Kholkine

Mestrado Integrado em Engenharia Eletrotécnica e de Computadores

Supervisor: Prof. Dra. Ana Aguiar

July 27, 2016

© Leonid Kholkine, 2016

Abstract

The number of cities that offer public wireless Internet on the urban buses is growing with the passing of the years. Porto's public city buses, through a joint-venture between Veniam, Porto Public Transport Society (STCP) and The Future Cities project, currently offer this service to its passengers.

It has been observed that users of mobile devices usually leave the wireless Internet on when they are on the street. In case that user had already used the wireless network of a public bus, the network will be memorised by the mobile device and connect every time it discovers it, even though sometimes the user might not be on the bus. In such case, the cellular connection will break and thus the wireless network will only be usable for a very short time.

This dissertation presents a study on if a mobile Access Point cam detect if the device tries to connect is on the bus. The dissertation focuses on an implementation of a mechanism which runs solely on the mobile Access Point, and therefore it was important to analyse of how the RSSI value can be used in tracking connecting devices and how the information from the GPS can additionally be integrated in that same mechanism.

By the end of this dissertation it is shown that the RSSI value is a poor indicator. However, by applying statistics on the data gathered in the bus, it is possible to correlate the speed of the bus and whether a connection is established inside or outside the bus.

Resumo

O número de cidades que oferecem internet sem fio nos autocarros públicos tem vindo a crescer nos últimos anos. Os autocarros urbanos públicos do Porto, através de uma parceria entre a Veniam, a Sociedade de Transportes Colectivos do Porto (STCP) e o projeto 'Future Cities', atualmente oferecem este serviço aos seus passageiros.

Tem se observado que os utilizadores de dispositivos móveis deixam a internet sem fios ligada quando estão na rua. Tem-se igualmente observado que caso já tenha utilizado esta rede sem fios, a rede será memorizada pelo dispositivo móvel e sendo assim vai se ligar cada vez que o dispositivo descobre a rede, mesmo se o utilizar não está no autocarro, desligando-se assim a internet da rede celular. Se o autocarro estiver a andar, o tempo de ligação vai ser de curta duração e será possível utilizar a rede sem fios durante um curto periodo de tempo.

Esta dissertação apresenta um estudo sobre como o ponto de acesso de Internet poderá detectar se o dispositivo móvel que está a tentar ligar está no autocarro. Foi escolhido implementar um mecanismo que funciona exclusivamente no ponto de acesso móvel, e por isso é importante analisar como é que o valor do RSSI pode ser utilizado para saber se o dispostivo móvel encontra dentro ou fora do autocarro. A informação do GPS também pode ser utilizada.

No fim desta dissertação, é possível perceber que o RSSI não é um bom valor para classificar se um utilizador esta dentro ou fora do autocarro. No entanto, foi encontrada uma correlação com a velocidade do autocarro, o que poderá ajudar no desenvolvimento de novas técnicas para melhorar a detecção destes casos.

Acknowledgements

This dissertation would not have been possible without the help and support of many people.

Before anyone, I would like to thank my adviser, Prof. Dra. Ana Aguiar, who helped me with developing my ideas for this thesis, providing valuable feedback, allowing me to learn many things that I wouldn't have learned otherwise and giving me all the conditions that I've needed to work at Instituto de Telecomunicações (IT). I would like also to thank everyone at IT who helped me with providing me advice and the tools that I needed.

Secondly I would like to thank everyone who has helped at Veniam - André Cardote who has been in touch with me through out the whole project and gave valuable support, Tiago Condeixa who guided me through the access point being used on the buses and Diogo Carreira for helping with collecting the data from buses.

I am very lucky to have several friends who helped me with this project - João Andrade who helped with C language when I was stuck, Dário Nascimento who gave some great ideas for my thesis and Ricardo Couto who helped me improve my Python code. A huge thank you to Pieter Coppens, Gert Willems, Mafalda Faria and Luís Gomes for proof reading this thesis.

Also I would like to thank my parents who have been a great support to me during my studies and the development of this dissertation. Without their support and love, I couldn't have done it!

Another group that is very important to me, are my friends who supported me during this thesis - They are so many that it's hard to list all of them in a A4 page, but you guys know who you are, and you rock!

Finally, I would like to thank for the usage of the icons in the figure of this dissertation from nounproject.com: "wifi" by João Proença, "Router" by Arthur Shlain, "Smartphone" by João Proença, "Bus" by Ilsur Aptukov, "Car" by Chang Kim, "Signal" by Joshua Soto

Leonid

"If you're not prepared to be wrong,
you'll never come up with anything original."

Sir Ken Robinson

Contents

List of Figures

List of Tables

Abbreviations

AP	Access Point
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EMA	Exponential Moving Average
FSPL	Free-Space Path Loss
GPS	Global Positioning System
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
OBU	On Board Unit
RFC	Ready For Comment
RCPI	Received Signal Strength Indicator
RSSI	Radio Signal Strength Indicator
STCP	Sociedade de Transporte Colectivos do Porto (Porto Public Transport Society)
SSID	Service Set Identifier
TIM	Traffic Indication Map
USB	Universal Serial Bus
WSN	Wireless Sensor Network

Chapter 1

Introduction

1.1 Context

Currently all the STCP public city buses in Porto offer free Internet to its passengers through WiFi hotspots which are connected to the city's vehicular network. This is done through a joint-venture between Veniam, STCP and The Future Cities project.

The WiFi on the STCP bus is an open network and uses the same Service Set Identified (SSID) among all the Access Points (AP) installed on all the buses. By having the same SSID any user with a mobile phone who has been connected once to the SCTP WiFi network will always connect as usually the mobile device memorises all the wireless networks by default. This means that if a mobile device has once been connected to the STCP WiFi Network, it will try to connect again even when it sees it, regardless of whether the user is inside or outside the bus - including pedestrians, passengers of other vehicles or anyone waiting at the bus stop. In case the mobile device that is outside the bus tries to connect, it will lose connection after the bus starts moving and the network becomes out of range.

1.2 Problem definition

1.2.1 Motivation

It is common for smartphone users to have the WiFi always turned on on the mobile devices. When having the WiFi on and the mobile device has the STCP WiFi network memorised, every time that a bus passes by the user, the mobile device will try to connect to the STCP network. Since the bus (and therefor the Access Point) is moving, the user will lose connection soon after. The implementation of the WiFi on the mobile devices isn't prepared for moving access points, most of the mobile devices will use a sticky hotspot strategy – The client does not disassociate from the current Access Point until there is an absence of connectivity for a predefined time period. That is why it can take significant time until the connection is again reestablished through the cellular network.

As some areas of the city have high frequency bus passages, this can have a negative effect on user experience.

1.2.2 Goals

The main goal of this thesis is to evaluate what is the impact of the problem described above is and propose a mechanism that avoids the connection of users which are not on the bus. This mechanism could be implemented on the On-Board-Unit (OBU - The access point installed inside the STCP bus), the user device or both. Said otherwise, this dissertation investigated how a Mobile Access Point can know if it is moving along with the client that is trying to connect.

The implementation on the user device is not very practical, as this depends on the user downloading and installing an application, requiring extra steps. The implementation of the mechanism only on the mobile hotspot could be achieved by reading the Received Signal Strength Indicator (RSSI) from the authentication and/or association packets. Other useful data that can be used is the GPS information, as this way we can know if the bus is moving or has moved and over which distance. Hence the goal of this dissertation is to understand the connection process and understand where and how a mechanism can be created in order to solve this problem.

1.3 Structure

Besides the introduction in this chapter, this dissertation has five more chapters. Chapter 2 contains a description of the important concepts and the related work. Chapter 3 describes the preliminary tests done in order to understand better the problem and an analysis of the RSSI value of a moving AP in a controlled environment. Chapter 4 shows the data that was gathered on the bus, how it was processed and the conclusions that can be withdrawn from it. In chapter 5 the proposed algorithm is explained and how to implement it on the moving AP. At last, chapter 6 summarises the conclusions of this work as well as presents the future work.

Chapter 2

Concepts and Literature Review

This chapter presents the review of useful concepts and related literature. First it describes the different stages that a mobile device goes through until reaching an established Internet connection on a WiFi network (discovery, authentication, association and obtaining an IP address through DHCP). A description of the RSSI value is presented, as at the moment it is the only main criterion that can be used in order to evaluate if a user is on the bus or not. The end of the chapter features the a summary of the different techniques that have been studied for understanding the position of a mobile device relative to an Access Point (AP).

2.1 AP Discovery Process

The communication done on IEEE802.11, also known as WiFi, in general is divided into 11 channels on different frequencies. Besides the 11 channels, more than one AP can use the same channel in order to communicate. The WiFi communication can also be done in two modes: The first is infrastructure mode, where an AP is the bridge between the users on the wireless network and the rest of the network. The second is the Ad-Hoc mode, where the users connect peer-to-peer. [1] In the scope of this dissertation only the information for Infrastructure will be shown, as this is the mode used on the STCP bus.

Before a connection can be established with an AP, the mobile device has to discover the existing WiFi networks that are available on each channel. Which is done through a process called scanning, and it can either be done either in passive or active mode.

In passive scanning, the device listens to each channel for a certain amount of time and registers information from any beacon frames it receives. The beacon frames are designed so that they have all the information in order to begin the information exchange between the AP and the client.

In active scanning, the device broadcasts probe request frames on each channel, and in case there is a network on that channel, it will reply with a probe response frame [2]. The figure 2.1 illustrates the behaviour of the scanning process.

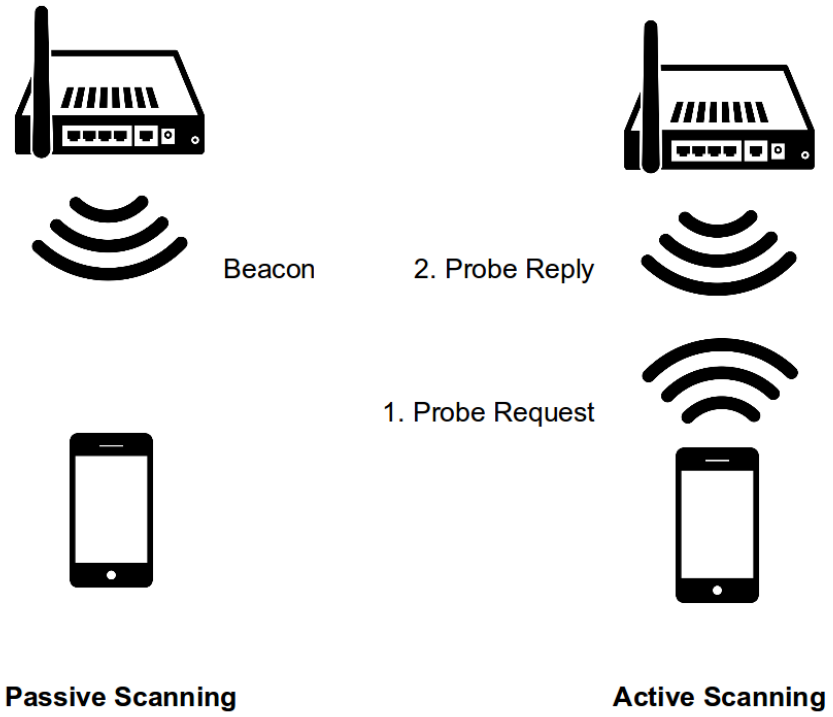

Figure 2.1: Passive vs Active Scanning

The scanning done in mobile devices (Android, iOS, ...) which is based on the implementation of each manufacturer, and the documentation is not very clear on when each scanning method is used. The mobile devices that were used for tests in this dissertation showed that when the WiFi was on, most of the time passive scanning was used.

The management frames that are used in the scanning process are described below.

2.1.1 Beacon Frame

The main use of the beacon frame is to keep the WiFi networks working and synchronized. The main information contained in the beacon frames is the following:

- Beacon Interval - The period in which the beacon frames are sent from the AP;
- Timestamp - Used to synchronizes the internal clocks of the devices connected;
- SSID - The identification of the network (known as the name of the network);
- Supported Rates;
- Parameter Sets - Contains the information about the signalling method used;
- Capability Information - Sends the requirements needed to connect to the network, for example, what type of authentication is used;

- Traffic Identification Map - TIM is used in order to signal the mobile devices that use the power saving mode that the AP has packages for them in the buffer.

The main functions of the beacon frames are to make sure that the network can be discovered, the internal clocks of the mobile devices are synchronized with the AP, and so that mobile devices that use power saving mode can know when they have packets to receive. [3]

Typically the beacons are sent approximately every 100 milliseconds, though this parameter is configurable on the Access Point. [4]

2.1.2 Probe Request and Reply Frame

The probe request frame is broadcasted during active scanning in order to discover known networks. A probe requests can be sent either to a specific SSID or it can include the broadcast address in the SSID field and receive the probe replies from all compatible AP on that channel.

The probe reply frame is similar to the beacon frame, except that it leaves out the TIM information, as the mobile device is not associated yet. [4]

2.2 AP Selection

The selection by mobile device of the AP to connect can be specific to the implementation of the manufacturer. One of the common criteria are the power level and the signal strength of the AP. [4]

According to the Android source code, more specifically in the file *wpa_supplicant.conf*, the selection criterion can be either based on the driver of the device or implemented by Android. Without knowing how the mobile devices select to which AP they connect, it is difficult to change parameters in order for the mobile devices not to select a certain network.

2.3 AP Authentication and Association Process

After the network has been discovered, there are three possible states for a mobile device to be in:

1. Not authenticated and not associated - While the mobile device decides whether to connect or not;

2. Authenticated but not associated - The user is authenticated to the network but is not connected to it yet;

3. Authenticated and associated.

The general process is described in the figure 2.2.

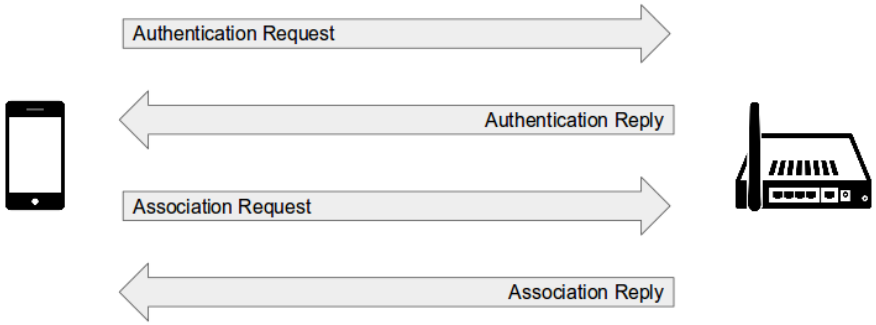

Figure 2.2: The Association Process

2.3.1 Authentication

All the information needed for the authentication process is included inside either the beacon or the probe reply. The authentication frames are used to make sure that the mobile device that is trying to connect has the authorization to do so.[4] There are several methods to authenticate a mobile device which will not be described here, as the STCP WiFi has an open authentication - Thus only two frames are exchanged:[5]

1. Authentication Request - Among other information, contains the ID of the the AP;
2. Authentication Reply - It can either authorize or reject the connection.

2.3.2 Association

After a mobile device is authenticated to the network, the mobile device has to associate itself to the AP, which is the equivalent of plugging in the network cable.[4] The association is also done with two frames: [5]

1. Association Request - The mobile device requests to be associated with the AP;
2. Association Reply - The association reply can either allow the association and return the association ID or fail the association request returning a status code. The criteria for allowing association or not depends on the different manufacturers.

The behaviour of the mobile device is not specified when the association is denied, and therefor the it will be tested in this work on different devices.

2.4 Obtaining an IP Address

After the device is associated to the AP, before communication can start, it needs to get the network configurations such as the IP Address, subnet mask and the DNS server. This information is

provided through the Dynamic Host Configuration Protocol described in RFC2131. There are 8 different messages that are sent on this protocol:

1. DHCP Discover - Sent by the client to locate DHCP servers;
2. DHCP Offer - Response from the server(s) with proposed configuration for the client;
3. DHCP Request - Sent by client (1) as a request to use one of the proposed configurations, (2) confirming if previous information is correct, or (3) extending the lease on a network address;
4. DHCP ACK - Acknowledging the request from the server;
5. DHCP NACK - The server signalling the client that the configuration is not correct;
6. DHCP Release - The client releasing the network address;
7. DHCP Inform - The client asking for the local configuration.

The process for acquiring an IP address is shown in figure 2.3. [6]

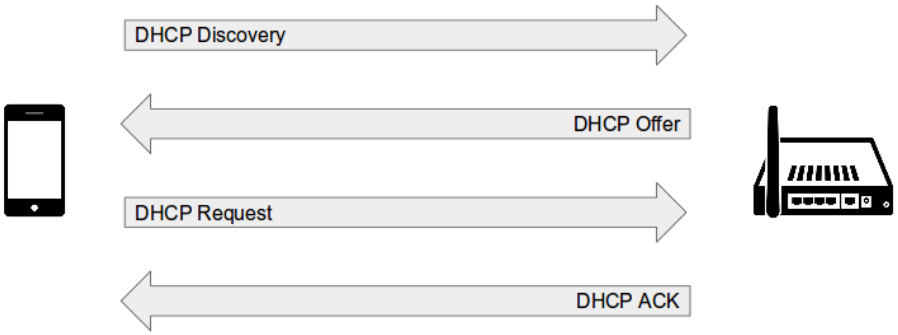

Figure 2.3: DHCP Information Exchange

It can also happen that the client has stored information (such as IP address from a previous connection), it can use DHCP Request to confirm if the configuration information is corrected, as shown in figure 2.4. [6]

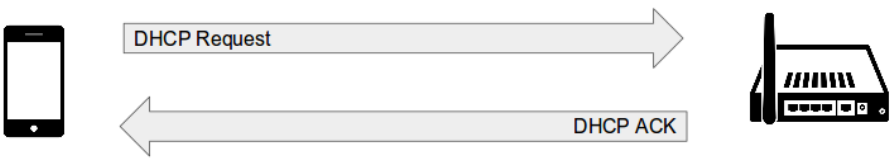

Figure 2.4: DHCP Configuration Confirmation

2.4.1 DHCP Delay

It has been shown that the DHCP process can take up to several seconds, especially in wireless networks.[7] This is due to two reasons. The first reason is the fact that the mobile devices consider the WiFi networks with the same SSID as the same network, therefor they will first try to renew the IP address in case the lease is still valid as shown in figure 2.4, though they will receive a NACK and will have to start the process shown in figure 2.3.[8]

The second reason is that the DHCP server performs a Duplicate Address Detection (DAD), to make sure that the address that the server wants to offer is not in use. This check is done by sending an ICMP ping to the network before sending a DHCP Offer. [8]

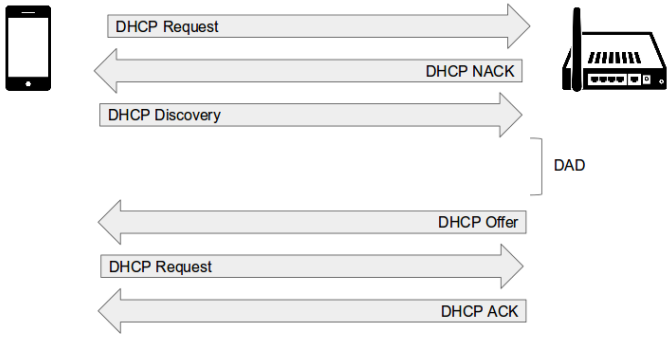

Figure 2.5: DHCP sequence diagram when the client has a previously acquired IP address

Therefor, the actual process of acquiring of the network configuration in case a client has a lease from another AP is shown in figure 2.5.

2.5 Estimation of distances using RSSI

Having GPS as a wide-spread localization methodology for outdoors, most of the research discovered on using RSSI localization has been focused on the indoors or for the Wireless Sensor Networks (WSN).

2.5.1 Description of the RSSI Value

G. Lui et al.[9] have shown that there are significant differences in the RSSI values among different WiFi devices, even if they are from the same vendor. This happens because each chipset maker can produce chips with different accuracy, granularity, range of the RSSI value and range of the power measured. On the other hand the RSSI value is only acquired from the preamble stage of receiving and not the whole frame is sampled, therefor having less data to have a more accurate measurement. In the IEEE802.11k-2008 standard[1] RSSI has been replaced by the received channel power indicator (RCPI) which improves some of the issues of the RSSI value, which includes the measurement of the data portion of the received frame and having a defined level of

resolution and accuracy. At the time of writing this thesis, the RCPI information was not easily accessible on the devices used for tests.

2.5.2 Free Space Model

The simplest way to calculate a distance based on the RSSI is using the free space model formula:

$$FPSL = 20log_{10}(d) + 20log_{10}(f) + 20log_{10}(\frac{4\pi}{c}) \tag{2.1}$$

In the equation:

- FSPL = Free Space Path Loss
- d = distance
- c = speed of light in vacuum
- f = signal frequency

This model is very simple and not very accurate. It has been shown that both indoors[10] and outdoors[11], the values are quite different compared to the real values - This is because the free loss path model doesn't take into account several factors, including as fading, shadowing and interference. [12]

2.5.3 Indoor localization methods

There are many methods that use the RSSI value as a localization method based. These methods include lateration methods, machine learning classification, probabilistic approaches and statistical supervised learning techniques. [12] These localization algorithms are empirical, based on locations which suffer less change and can have multiple fixed APs in order to improve the localization. These methods are not suitable for a larger scale outdoor environment, as there are too many changing variables.

2.5.4 Accuracy of the RSSI value as a localization parameter

Several studies [13] [14] show that even under optimal circumstances, the RSSI value on a simple elvel cannot be used reliably to measure a distance as the results aren't consistent among different conducted experiments.

Furthermore, K. Heurtefeux and F. Valois, explain that the value could be improved in under these conditions:

- Measure the RSSI value on different frequencies;
- Have a higher number of RSSI values in order to average decrease the variation;
- Have the clients with the emission and power and reception sensitivity calibrated;

- Have a high-quality antenna;
- Minimize the number of possible interferences (e.g., objects or rain);

All these conditions are impossible to implement in the scope of this problem, as it is not possible to have the controlled environment necessary. [14]

2.6 Summary

In this chapter the background information was presented which will be useful to understand in which stage the mechanism could intervene.

Even though there was research done on how to use RSSI in order to locate the device, this problem is very different, as the methodologies used indoors depend on the previous knowledge of the loss at the location. The outdoor environment can change much more compared to indoors (for example number of cars, number of passenger on the bus, other WiFi signals, ...). Having enough measurements in different points of the city in order to learn is not practical, as there would be too many points to measure. The research done on localization outside through RSSI shows that the parameter is not good enough and can vary greatly.

Some suggestions have been made in the related work on how to improve the RSSI reading, though those suggestions are not compatible with the problem at hand: There is a lot of random, uncontrollable variable in the environment where the measurements are made.

Chapter 3

Analysis of the Problem

To better understand the information described in the previous chapter, an analysis was done in order to see how the problem should be treated from the perspective of the mobile device and the AP. In this chapter, the behaviour of the mobile device inside the bus and outside the bus is characterized.

3.1 Introduction

For understanding if a device that is trying to connect is inside the bus or outside the bus, it is possible to use the RSSI value and the GPS information in order to make a decision. To understand what roles do these values play during the connection stage, it's important to characterize the connection time and location of the moving Access Point. The questions that are answered in this chapter are related to the moving AP and a stationary mobile device:

- If a mobile device is stationary and an Access Point is moving:
  - At which distance does the mobile access point connect? What is the RSSI when the mobile device connects?
  - How does the RSSI change when the device is connected to a moving AP?
  - At which distance does the RSSI disconnect from the AP?
  - How long is the mobile device connected to the AP when it is moving?
- How long does it take for a mobile device to connect outside and inside the bus?
- What are the RSSI values inside the bus?

Since the goal of this thesis is for the user not to lose the cellular connection due to the establishment of the WiFi connection, it is also important that the proposed solution does not allow the mobile device to connect when it is outside the bus. In this chapter different techniques that can deny a WiFi connection are analysed.

3.2 Moving Access Point

In order to answer the first set of questions described in the previous section, an experiment was setup with the same AP as from the SCTP buses. This AP was installed inside the a car and configured with the same parameters as the STCP bus. A Python script was running on the AP which recorded the RSSI and the position at the time. Besides the data recorded on the AP, an application was developed for the mobile device which synchronized clocks with the AP and recorded the time when the connection was established and lost. In order to ensure that data is always exchanged and the RSSI is updated through out the time, a continuous ping was executed every second. The following information was recorded:

- The timestamp of established connection and connection loss on the mobile device;
- The timestamp of the first and last transmitted ping;
- The RSSI at the corresponding GPS coordinates at a sampling rate of 1 second, as this is the rate at which the GPS information is updated on the mobile AP.

In order to ensure that the conditions do not change a lot, this experiment was done in the evening and in a straight street. The experiment is represented in figure 3.1.

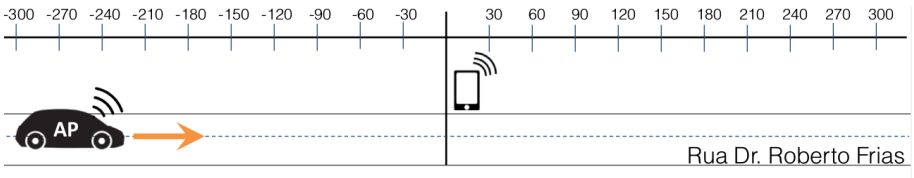

Figure 3.1: Experiment to characterise connection between a mobile device and a mobile AP

The mobile device was placed next to the bus stop. Four tests were conducted at an average speed that was 30 km/h, though due to traffic lights and other some other traffic, it was hard to maintain the same speed all the time. During the test the device was using an old IP address and only sending a DHCP Packet, therefor decreasing the connection time.

3.2.1 Connection to a moving AP

The distances at which the mobile access point connected and the RSSI values at connection are represented on figure 3.2. Looking at the distances between the mobile AP and the device, the connection was established as far as 300 meters away to as close as 20 meters. This is due to the behaviour described in the previous chapter: The android device performs a scan every 15 seconds, therefore the bus can be at different distances from the mobile AP when this happens. As consequence, the RSSI upon the first connection of the four tests was arbitrary.

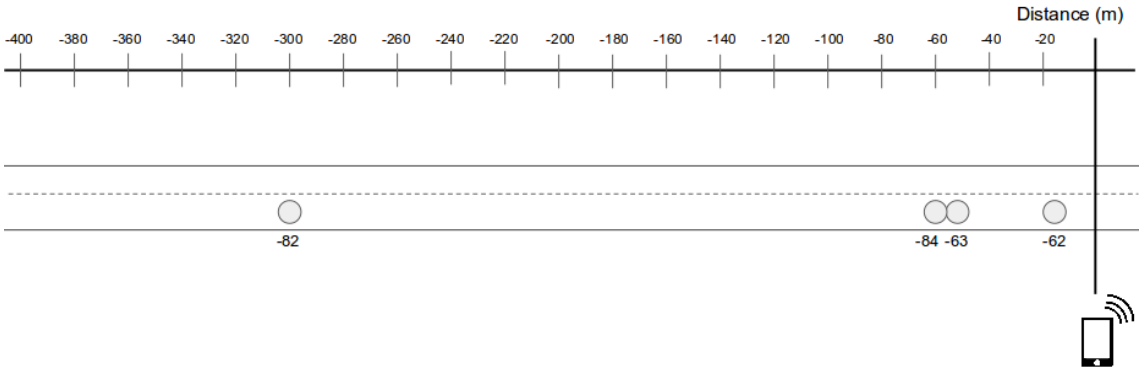

Figure 3.2: RSSI and the position during the connection to the moving AP

3.2.2 During the connection

During the connection the RSSI values were monitored and figure 3.3 shows the RSSI registered at different distances between the AP and the mobile device. It was observed that even with similar conditions the RSSI value varied in more than 20 dBm when close to the mobile device, on the other hand, the RSSI value was much more homogeneous when further away from the mobile device.

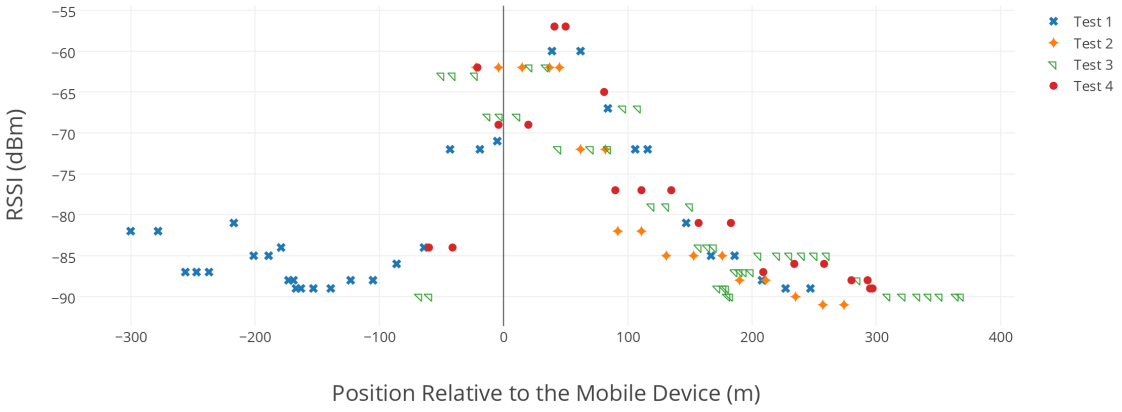

Figure 3.3: RSSI at different distances during the characterization experiment

The connection duration during the tests lasted from approximately 32 seconds to 64 seconds. The wide spread can be attributed to the traffic lights, but also to the differences in the connection timing.

Taking into account the result from the previous results, the duration can be separated into three periods:

- Connected - When the RSSI value is above -85dBm (less than 75 meters away);

- Poor connection - When the RSSI value is below -85dBm (more than 75 meters away);

- No Ping - Period of time when the packet does not receive any ping.

The boxplots for the times spent in each category is shown in figure 3.4.

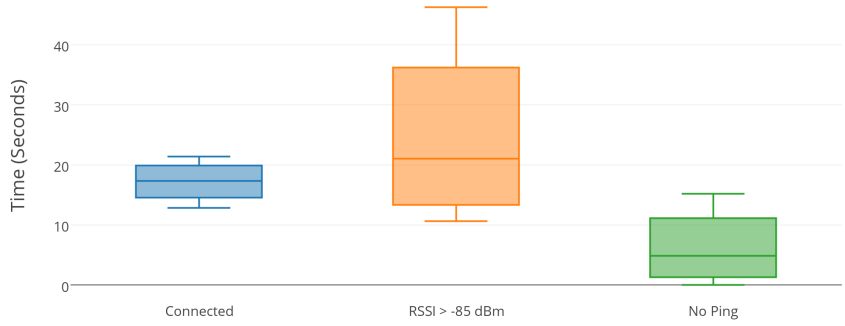

Figure 3.4: Time spent connected to the AP

It is possible to conclude from the initial tests that the stationary client spends a considerable amount of time with low RSSI value compared to when close to the AP. Regarding the total connection distance, during the tests the connection period never corresponded to more than 700 meters that the car has travelled.

3.2.3 Connection Loss

A closer look at when the device disconnected is presented on figure 3.5. It is shown that the mobile device took some time until it understood that the mobile AP is not in range anymore. The loss of connection happened from 240m to almost 300m from the mobile device. This shows that if a stationary mobile device connects to a moving AP, there will be some time that the devices isn't able to communicate at all with the AP.

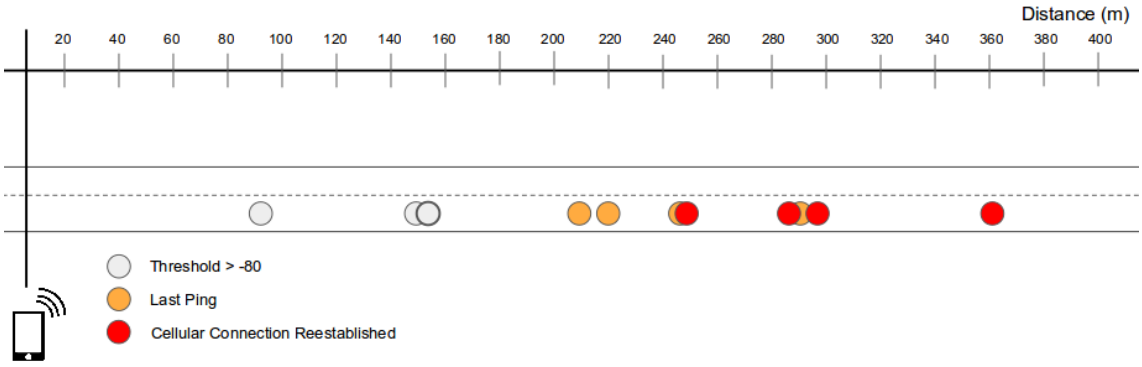

Figure 3.5: Distance from the client when connection is lost

3.3 Connection outside and inside the bus

In order to understand the difference between the connection inside the bus and outside the bus, a test was conducted inside and outside different buses. A mobile device was recording the amount of time each connection stage took and a laptop was capturing packets to understand what was happening. The experiment was always made with new a lease inside the bus and an old lease outside the bus to confirm the long DHCP timings as described in the previous chapter.

A summary of the connection time can be seen in figure 3.6. As expected the connection time is more homogeneous and takes less time inside the bus compared to outside of the bus. This is due to having more packets lost when outside the bus.

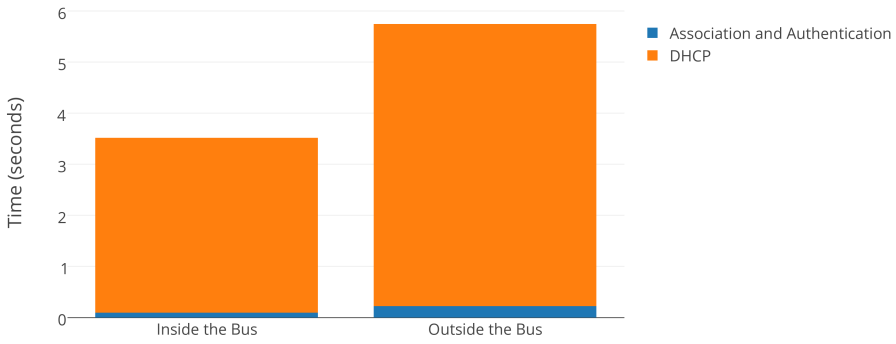

Figure 3.6: Average connection time inside and outside of the bus

This experiment also confirmed that during the connection, the DHCP process is the one that takes the most time. Figure 3.7 displays the packet captured for one of the connections when outside of the bus and shows the delay. It is possible to see that the mobile device takes 2 seconds

to send a DHCP Discover after the NAK and an aditional 2 other seconds for the AP to reply with a DHCP Offer to the DHCP Discover. In total, the whole process took 4 seconds.

```
705.949905  0.0.0.0      255.255.255.255  DHCP  397 DHCP Request  - Transaction ID 0x9eecb086
705.954631  10.1.95.1     255.255.255.255  DHCP  382 DHCP NAK      - Transaction ID 0x9eecb086
707.105869  0.0.0.0      255.255.255.255  DHCP  393 DHCP Discover - Transaction ID 0x1d929184
707.109532  0.0.0.0      255.255.255.255  DHCP  391 DHCP Discover - Transaction ID 0x1d929184
709.364840  10.1.95.1     10.1.95.97       DHCP  385 DHCP Offer    - Transaction ID 0x1d929184
709.369451  0.0.0.0      255.255.255.255  DHCP  405 DHCP Request  - Transaction ID 0x1d929184
709.373017  0.0.0.0      255.255.255.255  DHCP  403 DHCP Request  - Transaction ID 0x1d929184
709.376232  10.1.95.1     10.1.95.97       DHCP  385 DHCP ACK      - Transaction ID 0x1d929184
```

Figure 3.7: Demonstration of the DHCP delay

One important behaviour observed on the mobile device it is that the cellular connection was never lost while the device did not acquire an IP address from the AP. This means that from the user perspective, the WiFi connection is not established until the DHCP process is complete.

3.3.1 RSSI inside the bus

An analysis of the RSSI inside the bus was made with a customized application for an Android mobile device which recorded the connection duration and the RSSI values. It is important to note that the RSSI values that were recorded are captured by the mobile device and not the AP, and therefor can differ from the values read by the AP. There were 10 different tests done on each type of bus with a different number of passengers inside the bus. Each test was done for 30 seconds while sending a ping to the AP. The RSSI value was recorded in a normal and articulated bus.

The results can be seen on figure 3.8. It is possible to conclude that the RSSI values inside the bus, from the mobile device perspective, stay limited to a certain range. Even though more tests will need to be done with readings from the actual AP, it is possibility that inside the bus the RSSI values is limited to a certain range, and a criterion for not allowing to connect could be based on that range.

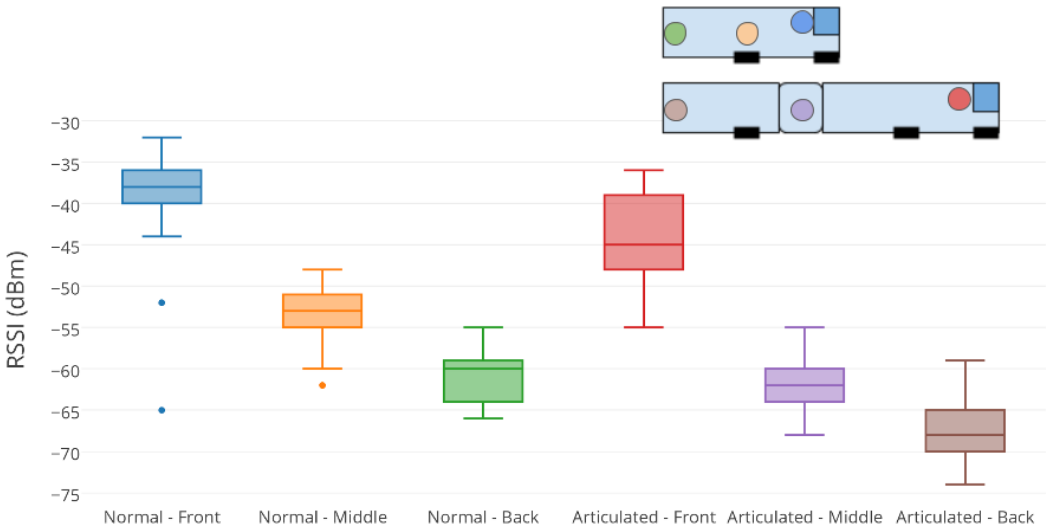

Figure 3.8: RSSI measured inside the bus

3.4 Android behaviour when denying a WiFi connection

The users that are outside the bus should not be allowed to connect to the WiFi network, therefor it is important to analyse the behaviour of the mobile device when it is denied a connection. As it was discovered during the previous experiments, the WiFi connection is established only when the mobile device has successfully acquired an IP address. Therefor the connection can be denied at three different stages: WiFi authentication and association, and the DHCP process.

In order to understand how a mobile device behaves when it is denied connection to an access point, a test was conducted on 3 smart phones with different Android versions:

- Lenovo Vibe Shot - Android 6.0.1
- LG Nexus 4 - Android 4.4.4
- Samsung S3 - Android 4.3

The test was conducted with modified version of hostapd that either did not reply to requests or denied them. During one minute, counting from the first authentication packet received, the timing of the packets was recorded and the duration between packets was calculated. The result can be seen in the figures from 3.9 to 3.13.

From the figures, it is possible to conclude that Android can behave very differently, depending on the mobile device used. When not denying an association request, while the Samsung S3 sends a packet every 4 seconds, the LG Nexus sends only 3 with a 30 seconds interval between the second and third packet. The best option to deny the connection is during the DHCP stage. Even

though it shows periods of up to 16 seconds, the behaviour is similar among the mobile devices - The time is increased between packets until a certain threshold is reached and afterwards it begins again from a lower value.

In any of the cases, the time between packets received when denying a connection is long and doesn't allow to sample different RSSI values, making its estimation more difficult.

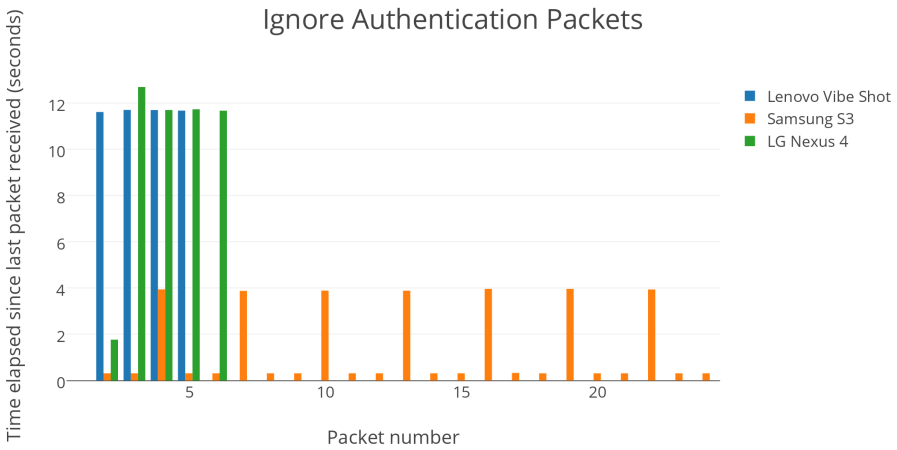

Figure 3.9: Packets resent when there is no reply to the Authentication Request

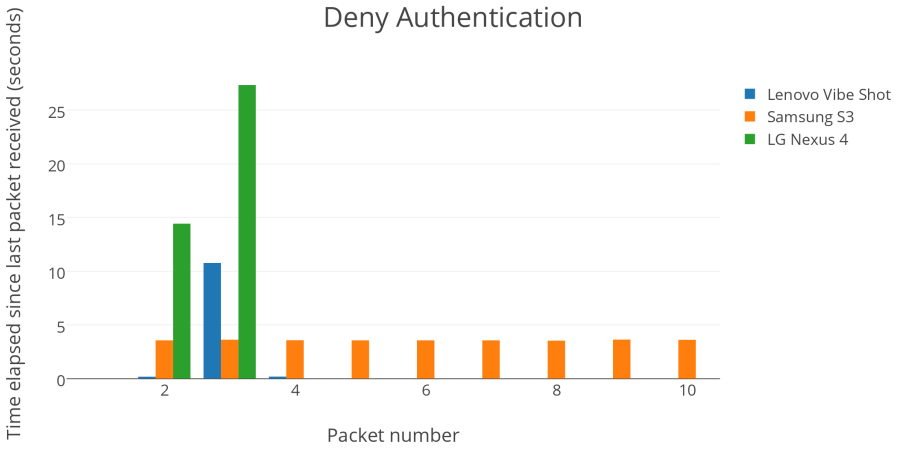

Figure 3.10: Packets resent when the Authentication Request is denied

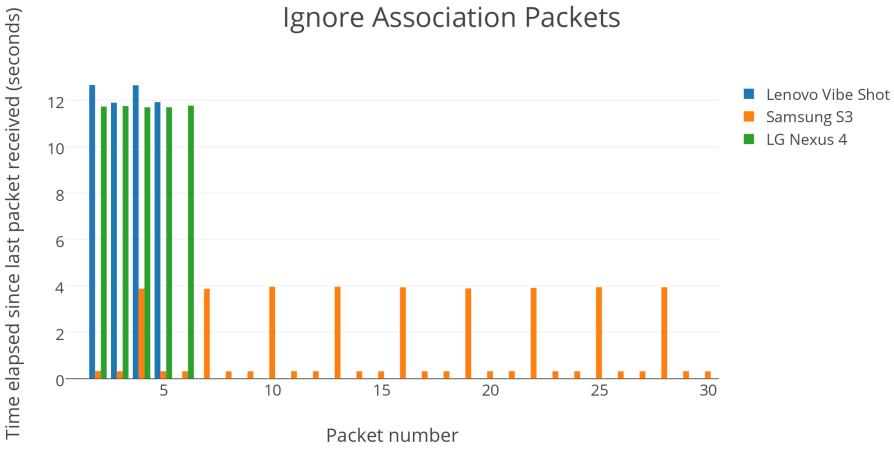

Figure 3.11: Packets resent when there is no reply to the Association Request

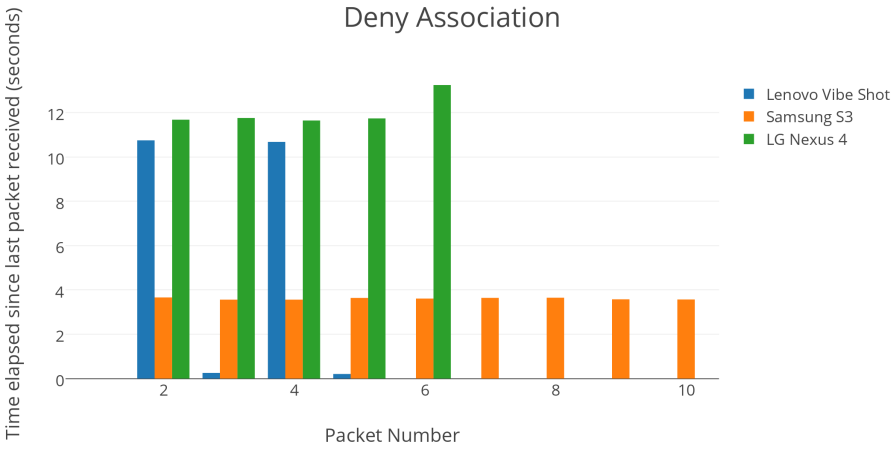

Figure 3.12: Packets resent when the Association Request is denied

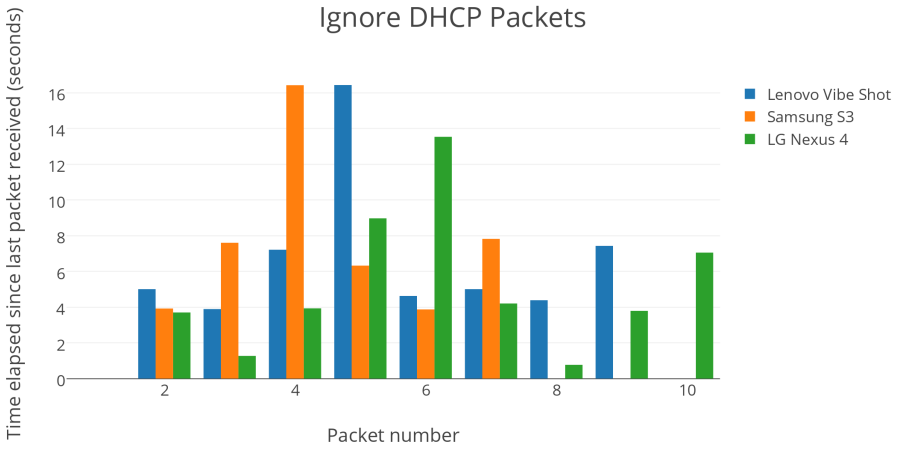

Figure 3.13: Packets resent when the DHCP packets are ignored

3.5 Summary

With this preliminary study and taking into account the related work described in the previous chapter, it is possible to conclude that the connection to a moving AP can happen at any distance from it due to the scanning period and the connection time outside the bus. Taking into the account the related work and the RSSI measurements, it is also not possible to know the concrete distance of the user based on the RSSI. Nevertheless, from the preliminary tests, it is possible to see that there could be a certain RSSI threshold that could possible determine if a mobile device is inside the bus or not. Another challenge that is for seen is that, as mentioned in the related work, in order to have a better RSSI value, it is needed an average from different packets. In this chapter it was shown that when denying a connection, there aren't many packets from which this average can be taken from.

Chapter 4

Data Collection and Analysis

In the previous chapter a characterization of the behaviour of the connection was done. The conducted tests in the previous chapter were done in a controlled environment and from those results it is impossible to generalise all the situations that can occur when a user tries to connect to the AP. In order to confirm the findings in the previous chapter and to support the decision making for whether a user is inside or outside the bus, it is important to collect and analyse data from the connection that happen on the STCP buses. This chapter describes the methodology, data segmentation and results from the data was collected.

4.1 Methodology

In order to make a proper decision if a mobile device that is trying to connect is inside or outside the bus, the following data was sampled every second for each connection on seven buses during one week:

- Timestamp
- MAC Address
- Average RSSI Value
- GPS Position
- Speed

The script was written in Python and acquired the RSSI information from the Linux command *iw station dump* and the GPS information from the GPS unit aboard the AP. The chosen frequency for registering data was one second, as that is the time when the GPS module refreshes the GPS information.

It is very important to add here that this data collection was performed on city buses in parallel with a commercial service operation. Thus the need to guarantee that the performance would not be impaired by your data collection. A simultaneous test was ran on 10 raspberry pi's with 2 WiFi

USB dongles connected to each. The raspberry pi's connected to the AP simultaneously on the 20 WiFi dongles to the mobile AP and downloaded a file of 1 Mb stored on the AP through a web server and the file download time was measured. The result is shown on figure 4.1. Different sampling periods were tested in order to understand if the script influences the performance of AP. The script showed no apparent influence from running on the AP.

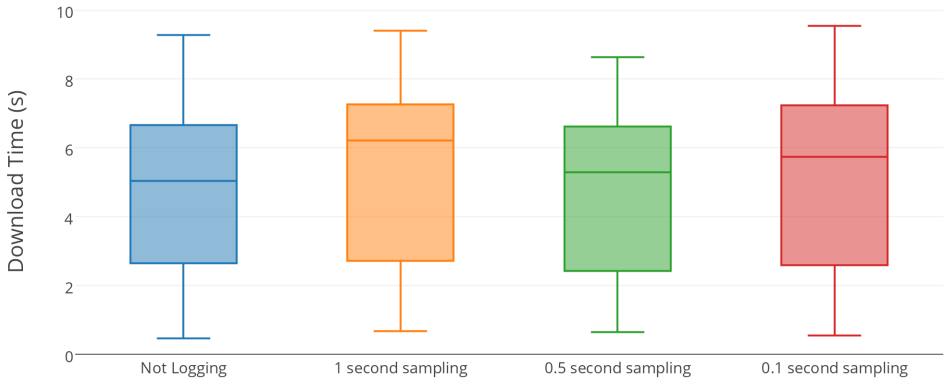

Figure 4.1: Performance test for test script

4.2 Data Gathered

The data was gathered from seven different buses during one week. The buses changed randomly the route every day. A connection was considered when the same MAC address appeared in the dataset with no more than 2 seconds difference between each other. In case there was a bigger difference of 2 seconds, it was considered as a separate connection. In total, around 5 million lines of data was gathered, which corresponds to 14063 total connections. For the purpose of the data analysis only the connections with at least 10 samples were considered. Also if the GPS failed (due to poor reception) during the connection, it was also discarded. This resulted in a dataset of 12040 connections. The table 4.1 summarises the data gathered. It's possible to observe on figure 4.2 where the connections occurred.

Table 4.1: Data gathered from the STCP bus

Data set	**Data points**
Original log file	4972424
Connections	14063
Valid Connections	12040

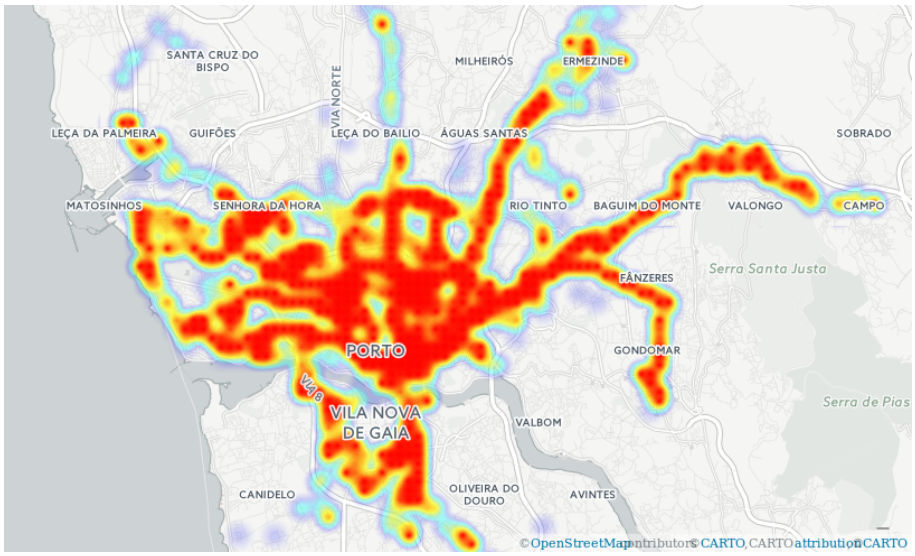

Figure 4.2: Geographical distribuition of the connections

4.3 Classification of the Connections

It is not possible to establish the ground truth if a connection is outside the bus or inside the bus. It was necessary to find a criteria to differentiate between the two types of connection. The decision was based on the distance travelled by the bus and the time that the device was connected. It was considered four different arbitrary thresholds: 250, 500, 750 and 1000 meters. For each of the categories, the outliers were removed using the Hampel identifier on the duration of the connection. The results for each groups are presented in figure 4.3.

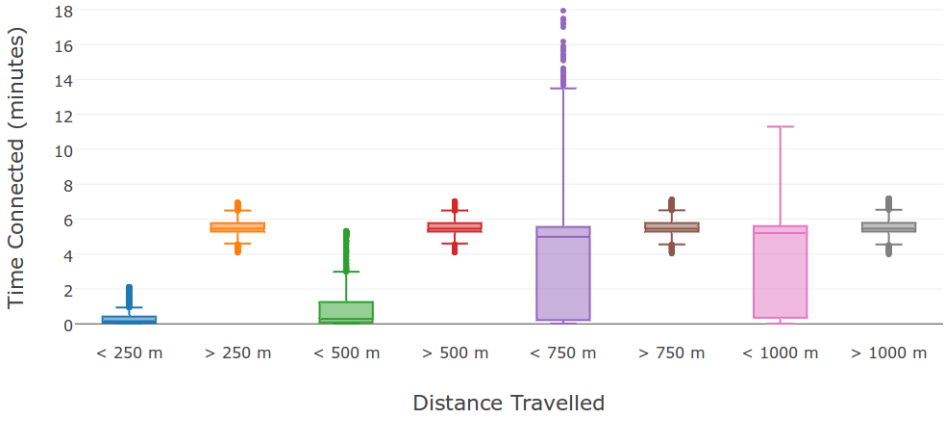

Figure 4.3: Data segmentation, inside vs outside the bus, for distances with outliers removed using the Hample identifier

The only group without any overlap in the time connected to the Access Point is the category of 250 meters. Therefor, two datasets were created: One for the connection where the total distance travelled by the bus was less than 250 meters and with a total connection duration between 20 seconds and approximately 2 minutes and one where the bus has travelled more than 250 meters with a total connection time between approximately 4 and 7 minutes. In total it was considered that there were 2350 connections outside the bus and 7400 connections inside the bus. The summary of the dataset is described in table 4.2.

Table 4.2: Dataset after detecting the outliers

Data set	**Data points**
Connections outside the bus without outliers	2350
Outliers of connections outside the bus	40
Connections inside the bus without outliers	7400
Outliers of connections inside the bus	2250

4.4 Analysis of the RSSI

The first step of the analysis was to study if the RSSI value was different among the connection outside and inside the bus. As there are many data points, the the mean, median and standard deviation during the first 20 seconds of connection was studied. Besides the RSSI value, also the EMA (Exponential Moving Average - Calculated by the Linux Kernel) was used as it gave an averaged value. When a user is outside the bus, there could be a bigger variation in the RSSI value, and therefor the mean, median and standard deviation of the RSSI variation was calculated. Finally, a linear regression of the RSSI value of each connection was also calculated to understand if there was an increase or decrease in the values.

To summarise, the following features were calculated for each dataset for the first 20 seconds of the connection:

- Mean of the RSSI
- Median of the RSSI
- Standard deviation of the RSSI
- Mean of the variation of the RSSI
- Median of the variation of the RSSI
- Standard deviation of the variation of the RSSI
- Mean of the Exponential Moving Average (EMA) of the RSSI
- Median of the EMA
- Standard deviation of the EMA

- Mean of the speed
- Median of the speed
- Standard deviation of the speed
- Slope of the linear regression of the RSSI
- Intercept value of the linear regression of the RSSI

Afterwards the measured information was visualized in boxplots. The RSSI mean and median can be visualized in figure 4.4. It is possible to see that there is no distinctions between the RSSI inside and outside the bus, therefor it is difficult to make a decision solely on the RSSI value. On figure 4.5 it's possible to see the mean and median of the variation of the RSSI. No conclusion can be drawn from this data if a user is inside or outside the bus, as both comparison don't present any obvious differences. The same can be said for all the features that have been selected. The rest of the features are presented in appendix A.

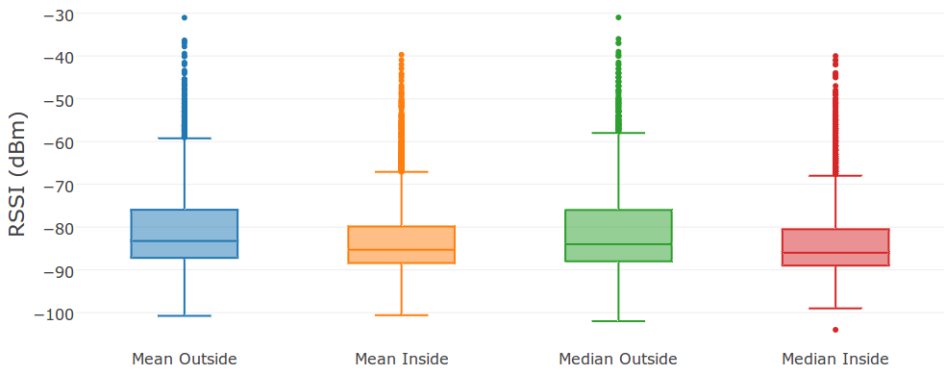

Figure 4.4: The RSSI mean and median

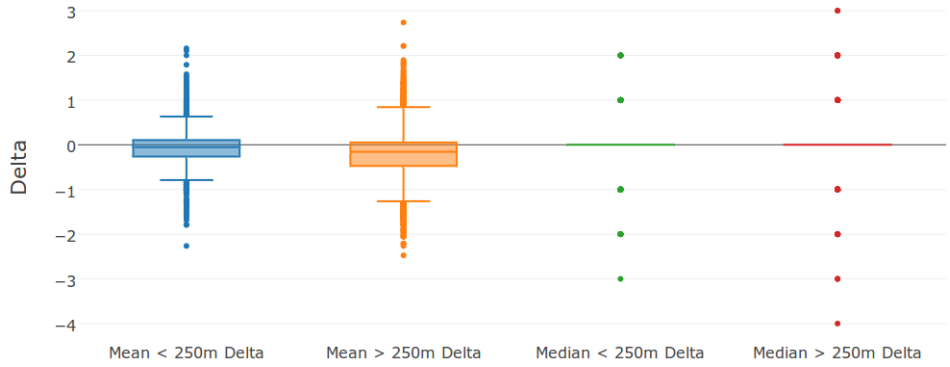

Figure 4.5: The mean and median of the variation of the RSSI

One of the reasons for the results presented above is that different devices could have different RSSI levels. Because the first half of the MAC address is assigned to the chipset manufacturer by the IEEE Standards Registration Authority (called Assignment), it's possible to analyse the RSSI median by manufacturer. In order to see the influence of the manufacturer on the RSSI level, the connection were grouped by the Assignment code and a boxplot of the median of the RSSI was traced. This trace can be seen on figure 4.6. Only the connections that travelled for over 1 kilometer of distance were included in the graphic, and only if there was more than 40 connection for the same assignment. From the figure it's possible to understand that there is a clear difference among the RSSI depending on the device that is used.

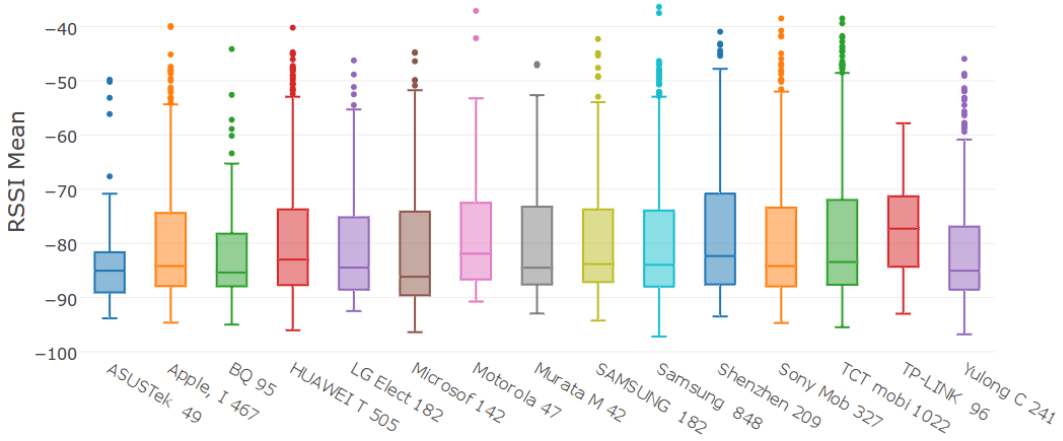

Figure 4.6: RSSI Values per Manufacturer

4.5 Bus speed during connection

In the previous section it was concluded that the RSSI value alone could not predict if a user is inside or outside the bus. The next step is to understand if the speed of the bus could somehow influence the decision. In order to study this to the previous features it was also added the mean speed during the first 20 seconds of the connection. As a decision tree helps us understand which features are important to destinguish if the users inside and outside the bus, it was decided to build a decision tree using the RapidMiner tool. Before creating the decision tree, the previous dataset was sub-sampled resulting in 2350 connections inside the bus and 2350 connections outside the bus. Afterwards the connections were split into 70% for training the decision tree and 30% for testing it.

After running RapidMiner, the decision tree on figure 4.7 was constructed. Even though the decision tree is very simple, it is very insightful, as it shows that the RSSI was completely discarded and only the speed feature was left. Another conclusion that is possible to take away it's that more connections outside the bus occur when the bus is moving slowly or not moving at all.

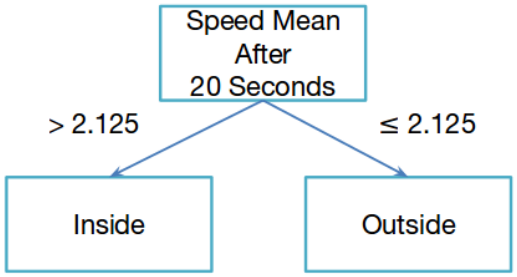

Figure 4.7: Decision tree after 20 seconds of connection

The big problem with using the data of after 20 seconds, it is that in the implementation of the solution, it will be necessary to wait 20 seconds before allowing connection. Therefor a new dataset was created with only the available information at the connection: The first RSSI value from the connection and the speed recorded at that moment. The same connections were used as previously. The result from RapidMiner is shown on figure 4.8. Again it is possible to observer that the RSSI value was completely discarded but the speed does play a role.

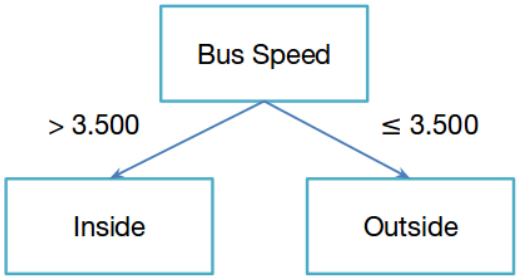

Figure 4.8: Decision tree with the initial information of the connection

For both cases described above the accuracy, true positive and negative rates are shown on table 4.3. The goal is to maintain the true positive rate high, as it corresponds to the number of users that are allowed to connect when they are inside the bus. From table 4.3 it is possible to conclude that just the initial speed does not present a good enough true positive rate.

Table 4.3: Sensitivity, Specificity and Accuracy of the decision tree with the initial information and after 20 seconds

	Initial Information	After 20 seconds
Inside the Bus (Sensitivity)	65.38%	81.22%
Outside (Specificity)	67.93%	61.31%
Accuracy	66.79%	71.41%

4.5.1 Speed of the bus before the connection

Looking at the decision tree that was generated, the speed mean and current speed are not completely zero. This means shows that the bus might have been moving before or after the outside connection. It is therefor important to answer the question - Could the speed of the bus before the connection influence the true positive and negative rates?

As only the speed during the connection was collected, it was necessary to extract the speed before the connection from other connections. A script in Python was written that is summarised in figure 4.9. An arbitrary time of 10 seconds before the connection was chosen. Afterwards a new dataset was created where the previous speed of the bus was available was created and the previous speed was added as a feature. The new dataset created is described in the table 4.4.

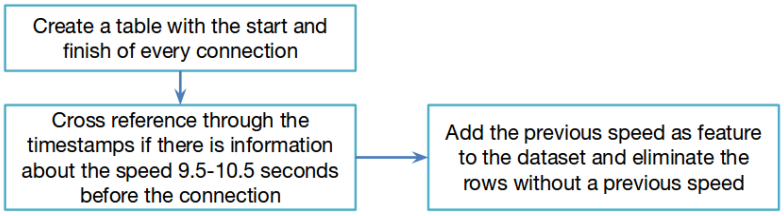

Figure 4.9: Algorithm for finding out the speed before the connection

Table 4.4: Dataset after detecting the outliers and searching for speed before connection

Data set	**Size**
Connections outside the bus	1301
Outliers of connections outside the bus	13
Connections inside the bus	5976
Outliers of connections inside the bus	1553

The same process was applied as previously to generate the new decision tree for both the initial information and after 20 seconds of connection. After 20 seconds of connection the decision tree remained the same but for the initial tree the previous speed was used as a criterion. The new initial decision tree is shown on figure 4.10. From the new decision trees generated it is possible to conclude that if the bus has just stopped (due to a higher value in the previous speed), it will influence the decision if the device that is trying to connect is inside the bus or outside the bus. This is not true after 20 seconds. It is possible that if the speed sampled with a different time before the connection, the criteria of the decision tree could change. The new accuracy, and true positive and negative rates are shown on table 4.5. The rates for the initial information are improved and due to using a dataset with less datapoints, the rates for after 20 seconds are changed though the accuracy is maintained.

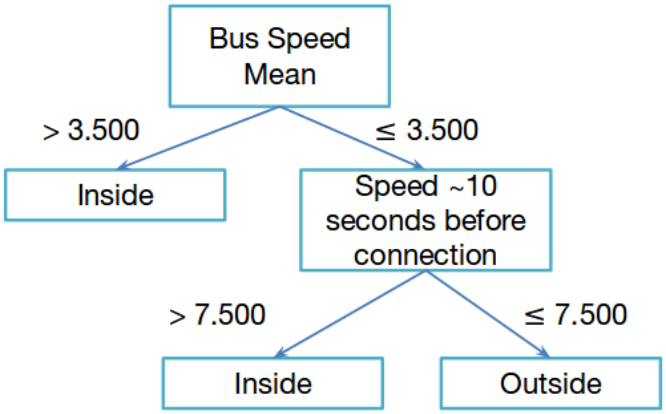

Figure 4.10: Decision tree for the initial information with the previous speed

Table 4.5: Sensitivity, Specificity and Accuracy of the decision tree with the initial information and after 20 seconds with the previous speed

	Initial Information (without prev. speed)	Initial Information (with prev. speed)	After 20 seconds (without prev. speed)	After 20 seconds (with prev. speed)
Inside the Bus (Sensitivity)	65.38%	73.59%	81.22%	87.44 %
Outside (Specificity)	67.93%	63.85%	61.31%	55.90 %
Accuracy	66.79%	68.72%	71.41%	71.67 %

4.5.2 Intervals for decision making

As mentioned previously, 20 seconds is a long time before deciding if a device should be allowed to connect or not. Therefor, an analysis of the speed mean 10 seconds and 15 seconds after connection was made. The same process for generating the decision trees was used and RapidMiner generated similar decision trees for each of the intervals. The summary of all the decision trees can be seen on figure 4.11. The parameters change over time, and it again confirms that if the bus has just stopped, it is more likely that is when the users outside of the bus will connect. The results for the accuracy, true positive and true negative rates are shown on 4.6. It is already possible to see that there is a tradeoff between the users that are on the bus and allowed to connect, the users that are outside the bus and not allowed to connect, and the time it is needed to analyse if the user is inside or outside the bus.

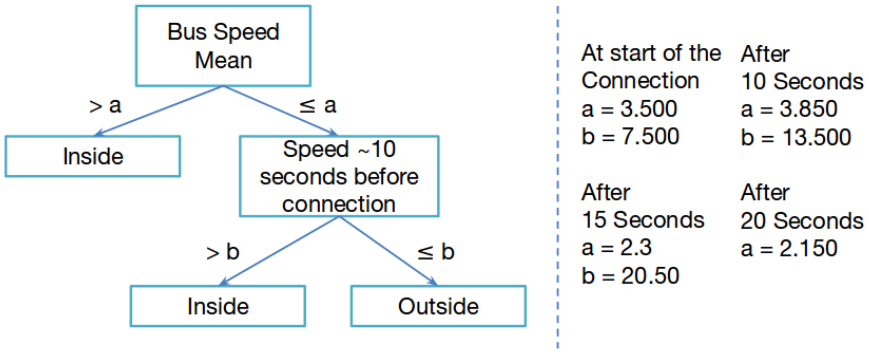

Figure 4.11: Summary of the decision trees generated for different time intervals

Table 4.6: Sensitivity, Specificity and Accuracy of the decision trees for different time intervals

	Initial Information	After 10 seconds	After 15 seconds	After 20 seconds
Inside the Bus (Sensitivity)	73.59%	80.77%	83.85%	87.44 %
Outside (Specificity)	63.85%	61.03%	56.92%	55.90 %
Accuracy	68.72%	70.90%	70.38%	71.67 %

4.5.3 Combining the decision trees

One possible solution to increase the percentage of the users that are inside the bus and are allowed to connect is to combine all the decision trees. That is, allow all the users that are considered on the bus to connect and wait for the next time frame to evaluate if the users that are considered outside the bus. In order to understand how this would decision, the diagram shown on figure 4.12 was ran in RapidMiner. The results for the percentage of the users that are allowed to connect or not is shown on the figure 4.13. With this technique it was possible to improve the true positive rate with the cost of waiting time for the user and decreasing the true negative rate.

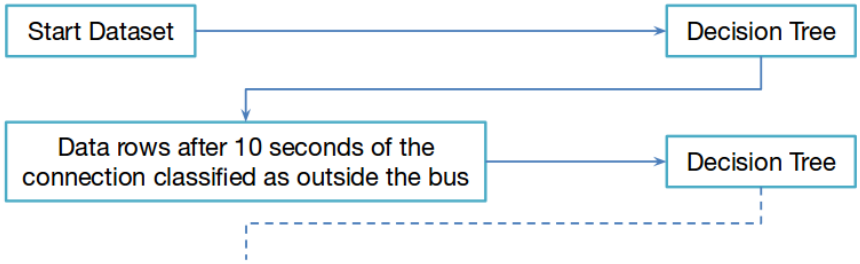

Figure 4.12: Data processing combining all decision trees

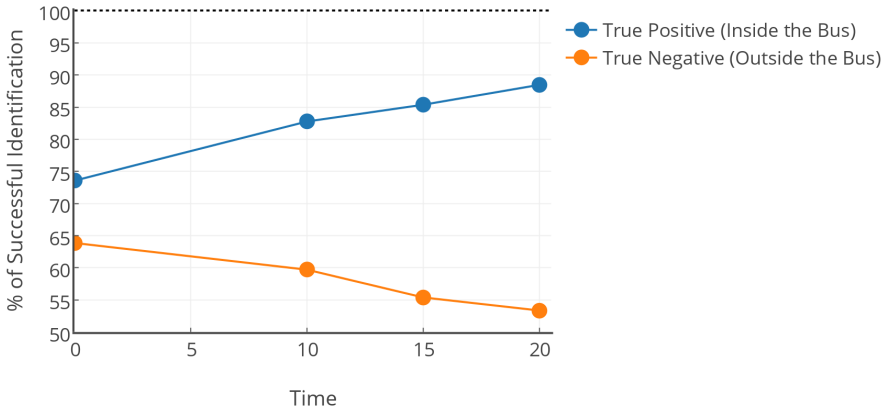

Figure 4.13: Data processing combining all decision trees

4.6 Summary

This chapter has shown, contrary to the was hypothesised in chapter 3, that the RSSI value is not a good parameter for evaluating if a mobile device that is trying to connect is inside or outside the bus.

On the hand, it was discovered that the speed of the bus (before connection, during connection and after the first connection attempt) could be a good criterion for making this decision. As seen in the previous chapters, a mobile device can take some time to discover a new network and in case it is outside the bus, also it could take some time until the connection is established. Therefor if a mobile device is outside the bus most likely it will connect when the bus stops.

The detection using the bus speed, according to the collected data, does present a tradeoff between the true positive rate (users that are on the bus and and get connected), true negative rate (users that are outside the bus and are denied connection) and the time it takes for the users to connect inside the bus.

Chapter 5

Mechanism for avoiding connections off the bus

Based on the results presented in the previous chapters, this chapter proposes a solution that is capable to run on the proprietary operating system of the access points. At the end of the chapter also the drawback of this mechanism are presented.

5.1 Description of the mechanism

As stated previously, the mechanism that is to be implemented on the mobile access point should evaluate if a mobile device is inside the bus or outside the bus before it is allowed to connect as for the user not to lose the cellular connection. This creates restrictions regarding on when this evaluation can be made. The study on when this can achieved is presented in Chapter 3.

As seen in Chapter 4, from the data collected, it is not possible to make a decision with a 100% certainty that when now allowing a connection the user is actually outside the bus. This means that this mechanism should also include a fallback timer. This is to ensure that if a mobile device inside the bus is classified as outside, it would be allowed to connect after a certain time.

5.2 Technical implementation

The implementation of the mechanism is done on a Linux based operation system. In order to manage the WiFi connection, hostapd is running on the router. For managed the DNS and DHCP, dnsmasq is running as well.

In order to deny the connection to a mobile device, it is possible to do so during authentication, association or the DHCP process. As described in Chapter 3, using DHCP to deny the connection is considered to be the best option, as the behaviour of the mobile device is more predictable. Therefor dnsmasq will need to be modified so that it makes a decision upon a reception of a DHCP packet.

The mechanism will also need to store the following information for it's usage:

- Monitored list: A list of MAC addresses that tried to connect and were not allowed to do so. This list also needs to record the time of the first connection attempt and the bus speed 10 seconds before the connection.

- White list: A list of MAC addresses that were trying to connect for longer than the fallback timer. MAC addresses on this list will be allowed to connect automatically.

- Bus speed: In order to know at which speed the bus was travelling before the connection and to calculate the mean, it is necessary to record the speed through out time.

As to keep the code in dnsmasq to a minimum, a parallel process will need to be running which records the speed and removes old entries from the lists.

5.3 Implementation on dnsmasq

The implementation of the mechanism in dnsmasq can be seen in the figure 5.1. Upon a DHCP packet arrival and before making a decision if a client is to be allowed to connect, dnsmasq needs to evaluate if all the conditions for making the decision are gathered. This means it should check if the speed monitor process is running, if there is enough information regarding the speed to make a decision and if the GPS readings for the speed are correct.

In case everything all the conditions for making a decision regarding the mobile device are gathered, the next step is to check if that device has been attempted to connect previously. In cast that it has not attempted, the initial decision tree should be applied as shown in the figure 5.2. In case that it has tried to connect, the first step is to check if the fallback period has passed. In case that it has not, then the other decision trees should be applied. As seen previously, a new DHCP packet can be received at any time. In this case the check should be performed +/- 2.5 seconds. This behaviour is shown in figure 5.3.

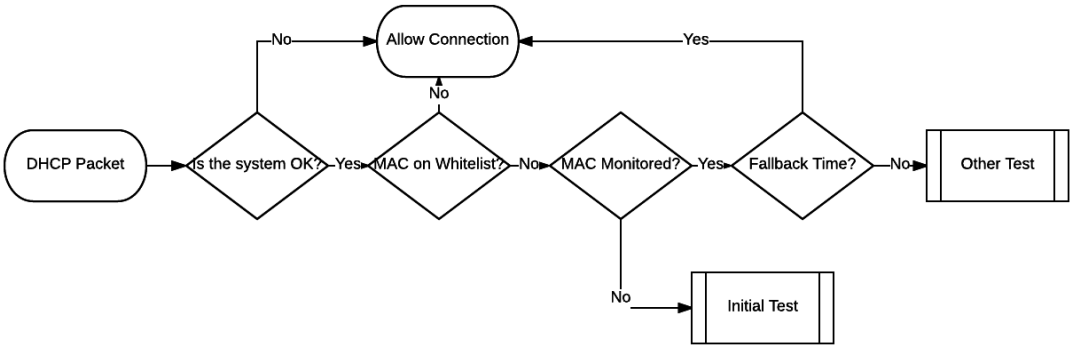

Figure 5.1: dnsmasq mechanism implementation

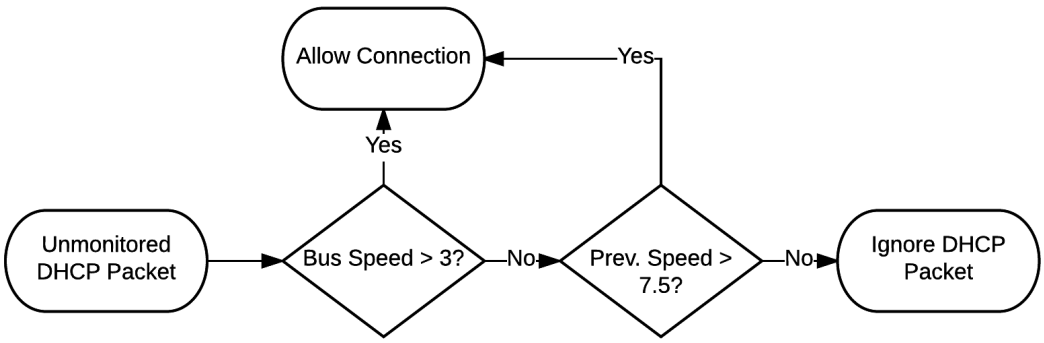

Figure 5.2: Process for first connection attempt

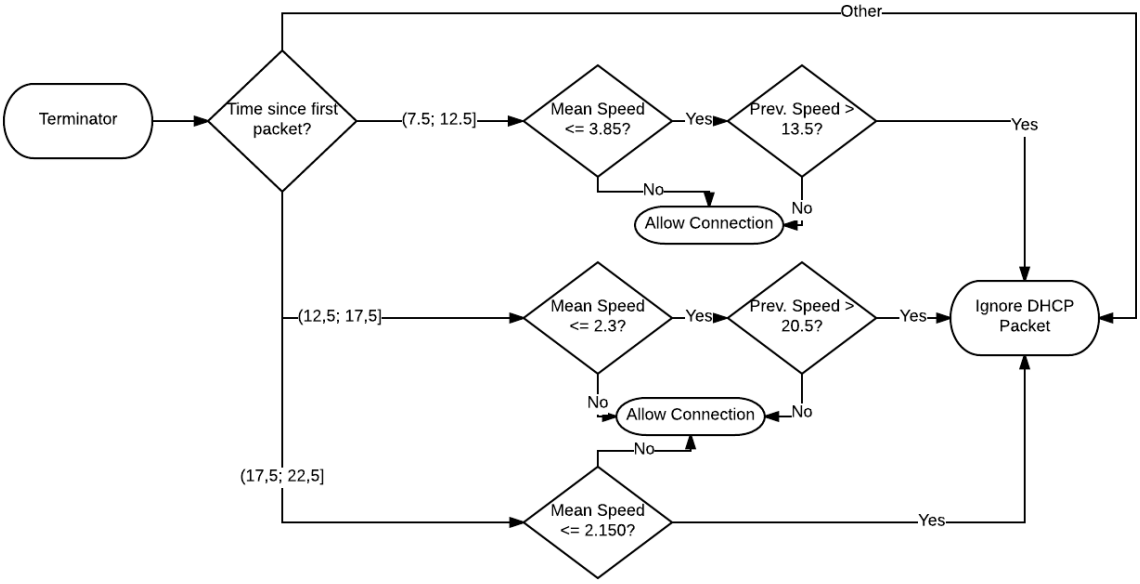

Figure 5.3: Process for other connection attempts

5.4 Bus Speed Monitor

Besides reacting to DHCP packets, the mechanism needs to register the previous bus speed values and to clean up the MAC tables. This is done through the monitor which flow work is represented on figure 5.4. The monitor registers the last 20 seconds of the speed, which allows dnsmasq to calculate the mean of the bus speed. This information is stored in shared memory. The MAC lists (monitored list and whitelist) is stored in a hash table and when the hash table is full it will empty the a percentage of the table.

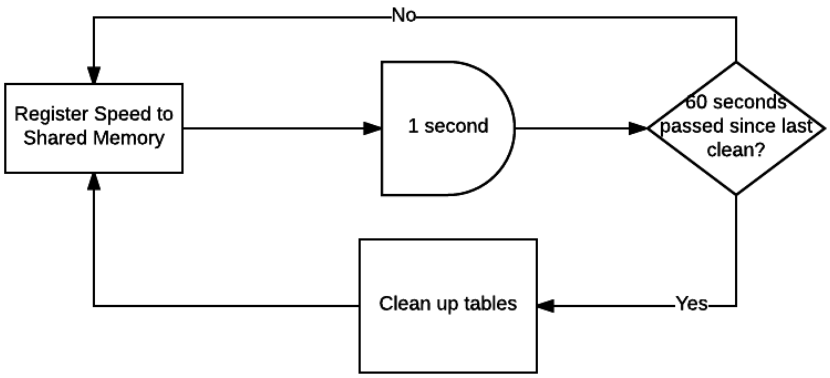

Figure 5.4: Paralel process for monitoring the bus speed

5.5 Mechanism Limitation

This mechanism presents limitations which are related to the trade-off presented in the previous chapter. The biggest limitation is that some user might need to wait up to 30 seconds before a connection is established, even if they are on the bus. Another limitation is that there could be an error in the estimation, as the DHCP packets do not arrive each second, and the decision parameters, at the moment, are only available for the first packet and after 10, 15 and 20 seconds of the connection. In the next chapter some improvements to this mechanism are presented as future work.

5.6 Summary

This chapter proposed a mechanism to detect connections inside and outside of the bus based on the data collected on the city buses. It uses the decision trees that were generated in the previous chapter. Besides implementing the decision trees, a fallback mechanism was included, as it is not possible to detect all the users that are inside the bus. At the end of the chapter the limitation for this mechanism were presented.

Chapter 6

Conclusions and Future Work

This dissertation explored the possibility for mobile access points to detect if the client that is trying to connect is moving along with it. In order to make this decision, the available information for making decision from the access point was the RSSI value and the GPS information. In the related work it is proven that the RSSI value is not a good localization parameter for the outdoor as there are too many unpredictable variables. Even though it is not possible to know the distance, for this work it was important to know whether there is a RSSI threshold which could distinguish the connections from inside or outside the bus.

As the outside environment can vary a lot, data was collected from different buses during one week. From this data it was possible to understand that it is not possible to distinguish using using the RSSI value if the a user is inside or outside the bus.

Afterwards a decision tree was created with features related to the mean of the bus speed and RSSI value during the first 20 seconds of the connections. The tool that was used to create the decision tree didn't consider the speed as parameter to distinguish connections inside and outside the bus, but it did consider the speed. A further study was done by adding as a feature the bus speed 10 seconds before and creating 4 datasets: With the information at connection time, after 10 seconds, 15 seconds and 20 seconds. It was possible to observe an improvement in the true positive and negative rates if the duration of the observation was longer and the information from the previous speed. It is possible to conclude from this result that a user outside the bus is more likely to connect when the bus has just stopped.

Using the results that are described above a mechanism which avoids partially the connections that are outside the bus was proposed. This mechanism is based upon the decision trees that were generated and includes a fall back period for the devices that are inside the bus but were not allowed to connect.

6.1 Future Work

Even though there is a tradeoff presented between the time that the mechanism waits before allowing the user to connect and the accuracy, the work presented in this thesis is a good step towards

improving the experience for the users that are outside the bus. In order to improve further the mechanism presented in this thesis additional data should be collected from the city buses and besides registering the data described here also register the bus speed in different intervals before the connection. For each connection the possibility of registering the RSSI directly from hostapd should be also studied. The mechanism could also be improved by studying the parameters for each time interval (that is, for 2, 3, 4, 5, ... seconds after connection).

During the data analysis, the connections outside the bus were mapped geographically and the result is displayed on figure 6.1. It is possible to see that there are many connections that happen in certain geographical area of the city. Those areas could be studied to further improve the decision criteria.

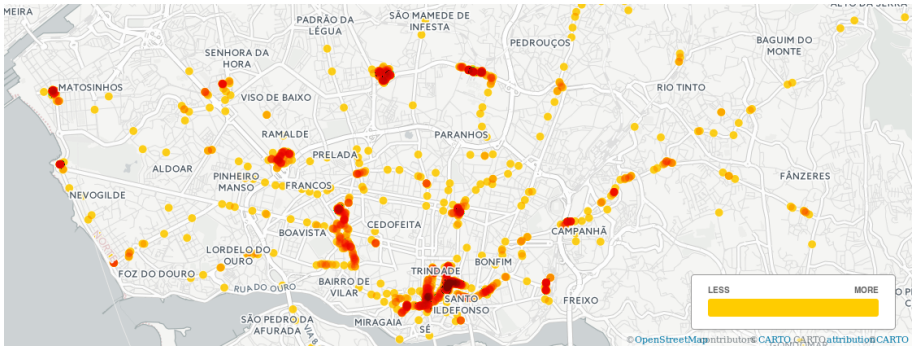

Figure 6.1: Geographical distribuition of the connections outside the bus

As there could be a long wait time for the user to connect to the access point, it is important to study how the connection time impacts the user. When a user boards the bus, he can take some time until he starts using the Internet and he will most likely wait in the queu to enter the bus, scan validate the transportation ticket and find a seat.

6.2 Contribuitions

Due to the specificity of the problem of this thesis, many tools were developed, including the following:

- Android application for measuring how long each phase of the connection takes time and logging the RSSI values during the connection;
- Python script for logging the GPS and RSSI information on the mobile access point;
- Several scripts to test the performance of logging script;
- Several python scripts for processing the data (aggregating the connections, eliminating the outliers, finding the previous speed of the connection, etc...);
- Partial implementation of the mechanism on the Access Point.

Appendix A

RSSI Values Measured inside the bus

In this appendix, all the graphics for RSSI values are presented.

The EMA value is the exponential moving average is calculated automatically by the Linux Kernel and displayed using the iw station dump command. It doesn't take into account the authentication and association management frames, as the iw station dump only shows the associated stations.

On all the figures below it is possible to see that there is no obvious difference which could distinguish the user inside and outside the bus based on the RSSI value.

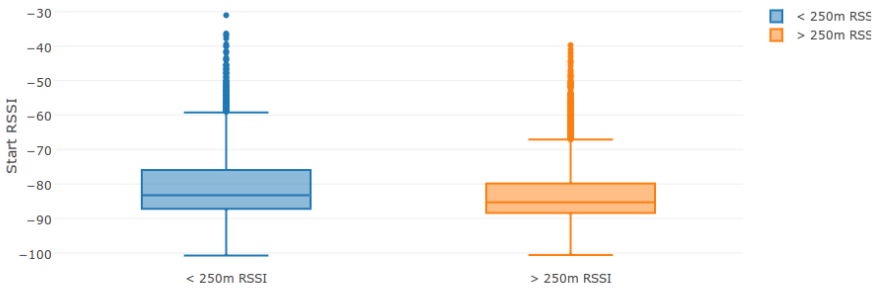

Figure A.1: The RSSI on connection

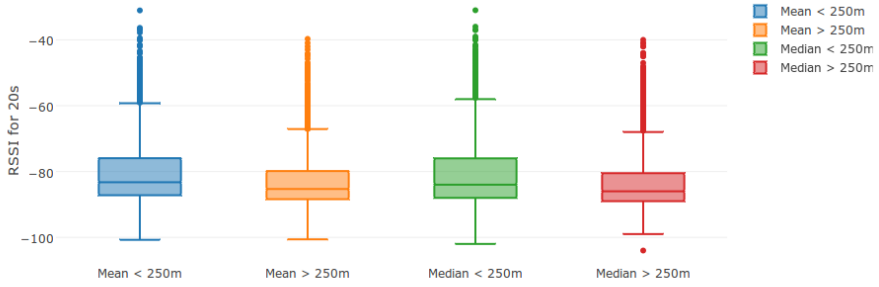

Figure A.2: The RSSI Mean and Median

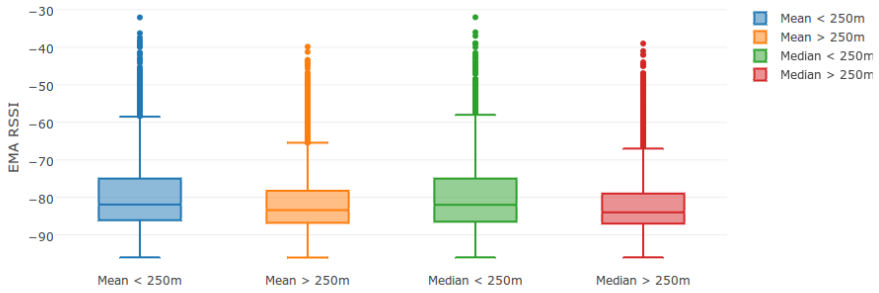

Figure A.3: The RSSI EMA Mean and Median

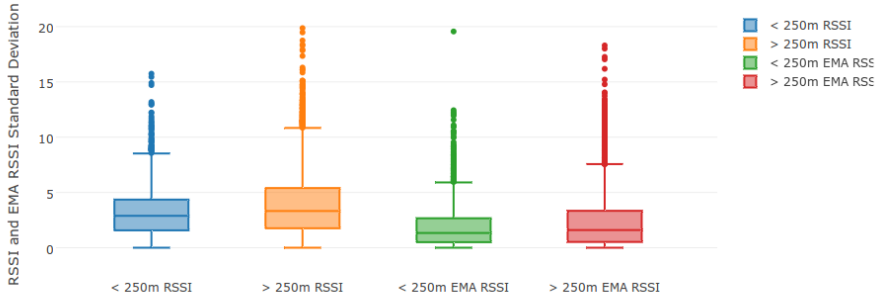

Figure A.4: The RSSI and RSSI EMA Standard Deviation

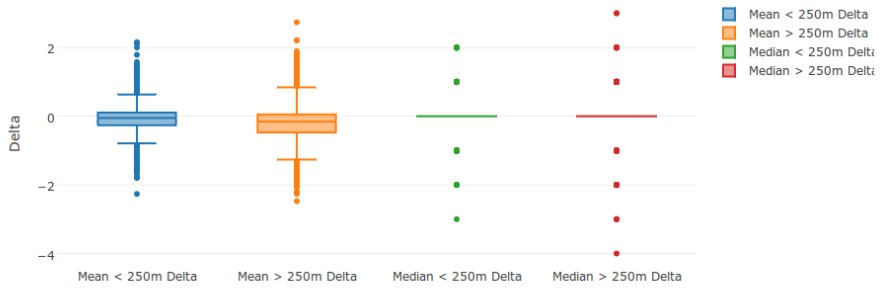

Figure A.5: The mean and median of the RSSI variation

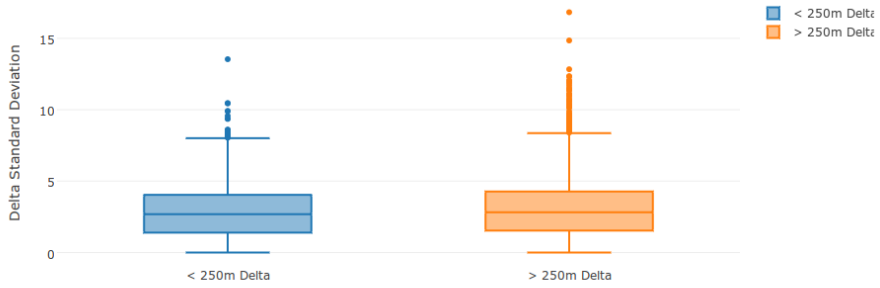

Figure A.6: The standard deviation of the RSSI variation

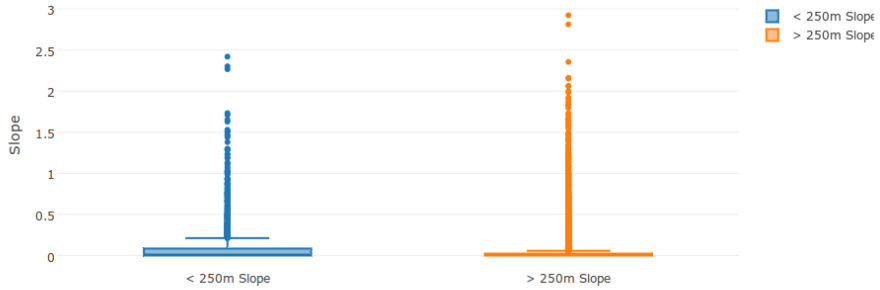

Figure A.7: Slope of the RSSI linear regression

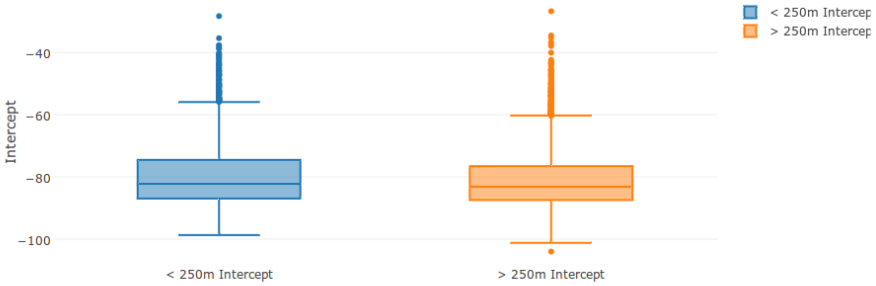

Figure A.8: The intercept value of the RSSI linear regression

References

[1] IEEE Standard for Information technology Telecommunications, information exchange between systems Local, and metropolitan area networks Specific requirments. Part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, March 2012.

[2] WiFi Alliance. Are are Passive and Active Scanning? http://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning.

[3] Jim Geier. 802.11 beacons revealed, October 2002. www.wi-fiplanet.com/tutorials/article.php/1492071/80211-Beacons-Revealed.htm.

[4] Matthew Gast. *802.11 Wireless Networks: The Definitive Guide*. O'Reilly, second edition, 2005.

[5] Intel. Understanding ieee* 802.11 authentication and association, April 2016. http://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000006508.html.

[6] R. Droms. Dynamic host configuration protocol, March 1997. https://www.ietf.org/rfc/rfc2131.txt.

[7] António Rafael Rodrigues Franco. Wifi roaming along urban routes, July 2014. Faculdade de Engenharia da Universidade do Porto.

[8] Sangho Shin Andrea G Forte and Henning Schulzrinne. Improving layer 3 handoff delay in ieee 802.11 wireless networks. In *Proceedings of the 2nd annual international workshop on Wireless internet*, page 12. ACM, 2016.

[9] G. Lui, T. Gallagher, B. Li, A. G. Dempster, and C. Rizos. Differences in rssi readings made by different wi-fi chipsets: A limitation of wlan localization. In *2011 International Conference on Localization and GNSS (ICL-GNSS)*, pages 53–57, June 2011. doi:10.1109/ICL-GNSS.2011.5955283.

[10] O. Katircioglu, H. Isel, O. Ceylan, F. Taraktas, and H.B. Yagci. Comparing ray tracing, free space path loss and logarithmic distance path loss models in success of indoor localization with rssi. In *Telecommunications Forum (TELFOR), 2011 19th*, pages 313–316, Nov 2011.

[11] W.A. Shittu, B.G. Bajoga, F. Anwar, and M.J.E. Salami. Prediction of received signal power and propagation path loss in open/rural environments using modified free-space loss and hata models. In *RF and Microwave Conference, 2008. RFM 2008. IEEE International*, pages 126–130, Dec 2008.

[12] R. Michael Buehrer Reza Zekavat. *Handbook of Position Location:Theory, Practice and Advances*. O'Reilly, first edition, 2012.

[13] Ambili Thottam Parameswaran, Mohammad Iftekhar Husain, Shambhu Upadhyaya, et al. Is rssi a reliable parameter in sensor localization algorithms: An experimental study. *Field Failure Data Analysis Workshop (F2DA09)*, 2009.

[14] K. Heurtefeux and F. Valois. Is rssi a good choice for localization in wireless sensor network? In *2012 IEEE 26th International Conference on Advanced Information Networking and Applications*, pages 732–739, March 2012. doi:10.1109/AINA.2012.19.